B29 Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing

Josiah Dykstra, PhD, 1739 Carriage Lamp Court, Severn, MD 21144*

After attending this presentation, attendees will be able to summarize the current integration of cloud forensic requirements into service level agreements (SLAs), and understand the international standards for cloud forensics. In particular, attendees will be able to understand how the Cloud Security Alliance mapped cloud computing to forensic standard ISO 27037 ("Guidelines for identification, collection, acquisition, and preservation of digital evidence").

Since the forensic process for cloud computing largely hinges on the legal contract between customers and providers, this presentation will impact the forensic science community by illustrating the Service Level Objects (SLO) that must be incorporated into service level agreements between customers and Cloud Service Providers (CSP).

In the short-term, the cloud consumer bears the responsibility to ensure that CSPs can respond appropriately to a forensic investigation. Consumers ultimately suffer the loss from crimes in the cloud environment. When contracting for cloud services, the customer should ensure that explicit language and SLOs are incorporated into the contract to ensure they can respond appropriately when the need to perform a digital investigation arises. For CSPs, integrating forensic capabilities into cloud offerings would increase transparency for the consumer and likely lead to greater revenue streams. As more organizations become reliant on cloud computing for critical operations, we foresee that forensics will become a key motivator on choice of CSP. Additionally, as the cloud market matures, legal and regulatory changes are forseen that may shift duties to include, collaboratively, CSPs.

ISO 27037 is an international standard that seeks to create a baseline for the practice of digital forensics.[1] Not intended to usurp local or national governmental authority, the standard's intent is to facilitate the usability of evidence obtained in one jurisdiction by a legal process operating in another jurisdiction. In its present form, ISO 27037 addresses identifying, obtaining and preserving potential digital evidence.

ISO 27037 is a relatively new standard (issued in October 2012) and only addresses the initial stages of a digital investigation, but it represents an international public and private sector consensus of how potential digital evidence should be handled in the critical initial steps of an investigation. There are many complex challenges of digital forensics in a cloud environment and how CSA mapped and reinterpreted the ISO 27037 guidance for a cloud context is explained.[2] For some parts of the standard, no changes are necessary for cloud environments. For others, including identification and acquisition of evidence, cloud requires special considerations.

References:

1. ISO 27037, Guidelines for identification, collection, acquisition and preservation of digital evidence. Available at http://www.iso.org/iso/catalogue_detail?csnumber=44381, 2012 [accessed 22 April 2013].
2. Cloud Security Alliance, Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing. Available at https://downloads.cloudsecurityalliance.org/initiatives/imf/Mapping-the-Forensic-Standard-ISO-IEC-27037-to-Cloud-Computing.pdf, June, 2013 [accessed 23 July 2013].

Digital Forensics, Cloud Computing, Forensic Standards

 ** Presenting Author*